

Long distance quantum communication over noisy networks

Andrzej Grudka¹, Michał Horodecki², Paweł Horodecki³, Paweł Mazurek², Łukasz Pankowski² and Anna Przysiężna²

¹*Faculty of Physics, Adam Mickiewicz University, 61-614 Poznań, Poland*

²*Institute for Theoretical Physics and Astrophysics, University of Gdańsk, 80-952 Gdańsk, Poland*

³*Faculty of Technical Physics and Applied Mathematics,
Gdańsk University of Technology, 80-952 Gdańsk, Poland*

The problem of sharing entanglement over large distances is crucial for implementations of quantum cryptography. A possible scheme for long distance entanglement sharing and communication exploits networks, whose nodes share EPR pairs. In [Perseguers *et al.*, Phys. Rev. A 78,062324 (2008)] an important isomorphism between storing quantum information in dimension D and transmission of quantum information in $D + 1$ network has been put forward. It implies that fault tolerant quantum computing allows in principle for long distance quantum communication. However, in fault-tolerant schemes, one usually considers creating known encoded states. However the process of encoding and decoding is exposed to error. We show that during this stage fidelity drops by a constant factor related to the volume of circuit that replaces a gate, while going to an upper level of concatenation. This shows explicitly, that it is possible to obtain long distance entanglement in $2D$ network. For $3D$ networks, much simpler schemes are possible, e.g. due to existence of Kitaev topological quantum memory, which uses $2D$ lattice. Again, we consider explicitly the encoding and decoding stages. In [Dennis *et al.* J. Math. Phys. 43, 4452 (2002)] such scheme was provided in terms of gates. Here we propose a very simple scheme, based solely on syndrome measurements. It is then showed that the scheme is equivalent to teleporting the state to be encoded through some virtual EPR pair existing within the rest of qubits. We then present numerical simulation of performance of such encoding/decoding scheme.

I. INTRODUCTION

Suppose we have network of laboratories with some fixed distance between neighboring ones, and one of them wants to establish quantum communication with some other lab. We assume that the neighboring labs can directly exchange quantum communication with some small, fixed error. This can be used e.g. to share some noisy EPR pairs between such neighboring labs. We also assume all the operations performed within each lab may be faulty with some fixed, small probability. If with the help of all labs, two distant ones can achieve quantum communication, they can exploit it to share cryptographic key, that will not be known to other labs in the network (even though they participated in its creation). This scenario put forward in [1], an alternative to quantum repeaters [2, 3] is closely related to entanglement percolation [4], and may be crucial to increase the distance of quantum communication beyond the present capabilities which are now of order of hundred kilometers. Note that if quantum communication over distant nodes is established, one can also share entanglement, by sending one qubit from entangled pair to one distant location, and the second one to the other location.

In [1] the question was posed whether for two dimensional network, in principle, one can perform quantum communication over arbitrary distance, provided that the size of the systems in each node is constant, i.e. it does not depend on the distance. The answer was affirmative. Namely, the authors first represented quantum computation on line as a teleportation process on quantum networks. Then, they referred to the result of [5] where a scheme for universal fault-tolerant quantum computing

was designed.

There is one issue though, which was not discussed in [1], and will be considered in this paper. Namely, in fault-tolerant schemes, one typically starts from known logical states, which can be then fault tolerantly stored. In such case, the above idea offers entanglement between two logical qubits, which are distributed among many nodes of the network. We would simply have entanglement between two faces of the square networks rather than between two nodes. However, this does not allow to share key between two users of the networks (i.e. two nodes of the network). To achieve this, one could need to be able to store an unknown state of a single, physical qubit.

The crucial point is the stage of encoding this single qubit into logical qubit; this cannot be done with arbitrarily large fidelity [6], because at least at the very first step, the qubit is exposed to noise (as it is not encoded yet). However, assuming that it is possible to maintain reasonable fidelity, during encoding stage the state can be further stored virtually without any loss. Passing to the network picture, we would obtain, that an unknown qubit can be then transmitted from one node to other distant node, at a fidelity, essentially determined by the fidelity of encoding and decoding stage. To share entanglement, at a fixed node, two qubits are prepared in entangled state, and then the qubits are propagated into opposite direction (i.e. each one is encoded and then transmitted in encoded form).

One can consider an alternative way, which does not use encoding of unknown qubits, but only decoding. Namely, if we have entanglement between faces, we can then use decoding stage, to concentrate it to single qubit.

Let us mention here that in [7] it was shown, that entanglement between two faces of 3D network can be obtained. Also in [8] a scheme of transmitting qubit over long distances in 3D based on cluster states was provided.

In this paper we show how to transmit qubits between distant nodes of 2D network. To this end we provide explicit estimate for fidelity of encoding/decoding of unknown state in fault-tolerant scheme. Secondly, we provide a very simple scheme of transmission qubits between distant nodes in 3D using Kitaev toric code. Our main result here is a scheme of encoding/decoding a qubit in unknown state into Kitaev 2D code solely by measuring syndrome operators, measuring and preparing qubits in bit and phase bases, and correcting the qubit by bit and phase flips at the end of decoding stage. This latter operation usually is not needed, e.g. when we want to use the communication to share secret key. This is an improvement over a more complex scheme of encoding/decoding presented in [6], and implies for a conceptually simpler scheme of quantum communication by use of 3D networks, including entanglement percolation at a constant error rate. We also present our encoding/decoding scheme as a kind of teleporting the qubit into and out of the code.

The paper is organized as follows. In Sec. II we analyze storing a physical qubit by means of fault tolerant scheme. We give estimate for fidelity of encoding process. In Sec. III a simple scheme of protecting physical qubit by means of Kitaev code is proposed. We then identify the encoding scheme as teleportation in Sec. IV. Finally, we provide simulations of performance of the scheme in presence of noise in Sec. V. Finally the implications of our results on communication over long distances by use of EPR networks is discussed in Sec. VI.

II. QUANTUM COMMUNICATION OVER LONG DISTANCES BY USE OF 2D NETWORK

In [1] it was shown how computing on d dimensional lattice that uses solely local gates can be mapped onto single shot action on EPR network of dimension $d + 1$, where only local operations are performed and classical information can be exchanged. Therefore to send a qubit from one node to another node of such a network is equivalent to storing a qubit by means of some quantum circuit on network of smaller dimension.

Here we will present a scheme, where we start with physical qubit $a|0\rangle + b|1\rangle$ and encode it by use of fault tolerant scheme in 1D based on concatenation. (There exist schemes that consist of local gates [5]; actually any scheme, which uses a code that can correct more than two errors, can be changed into local at the expense of lowering the noise threshold value). We will now estimate fidelity of reaching a given level of concatenation r . The total fidelity is then given by product of fidelity of encoding F_{enc} , fidelity of decoding F_{dec} and fidelity of storage of encoded state $F_{storage}$. The latter is arbitrar-

ily good, exponentially in size of code ($=2^r$), and we can assume that $F_{enc} \leq F_{dec}$ (this happens for fully unitary fault-tolerant scheme as e.g. in [9], and if we do not need to perform correction, as is the case in cryptographic applications, F_{dec} is larger than F_{enc})

Suppose v is the volume of the physical circuit (i.e. the number of gates, including identity gates) which encodes into a logical qubit of first concatenation level. The probability of success of this encoding stage is then larger than $(1 - p)^v$ where p is probability of error per gate. Indeed, if any element of our circuit will work – which happens with probability $1 - p$ – then, the output will be correct. In next encoding stage, the effective probability of error per logical gate is $p_1 \geq cp_0^2$, where c is number of pairs of locations of the circuit, i.e. $c = \binom{v}{2}$, and $p_0 \equiv p$. Thus, the probability of success of encoding into second level of concatenation is no smaller than $(1 - p_1)^v$. The probability $p_s^{(r)}$ that we pass successfully $r + 1$ stages is a product of such probabilities in each stage, hence we have

$$p_s^{(r)} = (1 - p_0)^v (1 - p_1)^v \dots (1 - p_r)^v \geq \prod_{k=0}^r \left(1 - \frac{1}{c} (cp)^{2^k}\right)^v. \quad (1)$$

We now proceed to estimate this from below. Using notation $\alpha = 1/c$, $\beta = cp$ we obtain

$$\frac{1}{v} \ln(p_s^{(r)}) = \sum_{k=0}^r \ln(1 - \alpha\beta^{2^k}) \geq \int_0^{r+1} \ln(1 - \alpha\beta^{2^x}) dx \quad (2)$$

Extending the limit to infinity and changing variables, we obtain

$$\frac{1}{v} \ln(p_s^{(r)}) \geq -\frac{1}{\ln 2} \int_0^\beta \frac{\ln(1 - \alpha z)}{z \ln z} dz. \quad (3)$$

Since we assume that $cp < 1$ (otherwise the concatenation scheme would be useless), the integrated function $f(z) = \frac{\ln(1 - \alpha z)}{z \ln z}$ is monotonically increasing, so we can estimate the integral by just $\beta f(\beta)$, obtaining

$$\frac{1}{v} \ln(p_s^{(r)}) \geq -\frac{\ln(1 - p)}{\ln 2 \ln(cp)} \geq \frac{p}{\ln 2 \ln(cp)} \quad (4)$$

where we used $\ln x \leq x - 1$ for all $x \geq 0$. If $cp \leq 1/e$ which is only slightly stronger than the fault-tolerant threshold assumption $cp < 1$, we obtain

$$\frac{1}{v} \ln(p_s^{(r)}) \geq -p \quad (5)$$

We have thus obtained the following result

Proposition 1 *If error rate p satisfies $p \leq p_{th}/3$ where p_{th} is threshold for error rate in fault-tolerant architecture based on concatenated codes, then the fidelity of encoded state satisfies*

$$F \geq e^{-pv} \quad (6)$$

where v is the volume of encoding circuit on physical level.

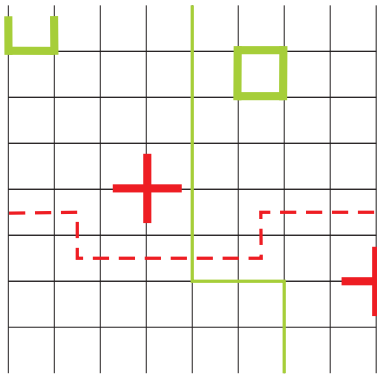


FIG. 1: Planar code. A code space is given by eigenvectors of all star and plaquette operators with eigenvalues $+1$. The lines represent exemplary logical X (dashed line) and Z (solid line) operators on code space. They are given by homologically nontrivial loops, i.e. ones connecting opposite boundaries in, the original and dual lattice respectively. Otherwise, the loops can be chosen arbitrarily. The codeword $|0\rangle_L$ is superposition of all standard basis vectors, with configurations of 1's (treated as a set of paths in dual lattice) being homologically trivial. The codeword $|1\rangle_L$ superposition of all vectors with non-trivial configurations. The homology is determined by the number of paths of 1's crossing the green line, i.e., we have even number when homology is trivial and odd number when it is nontrivial, which in turn determines the sign of the logical observable Z .

III. SIMPLE SCHEME FOR ENCODING AND DECODING QUBIT FOR KITAEV CODE

A disadvantage of the fault tolerant schemes based on concatenated codes is that they are usually quite complex. Originally, it involves non-local gates (i.e. ones which do not connect next neighbor qubits). There are methods to convert any nonlocal scheme into a local one, though this significantly increases complexity of the scheme.

A much simpler scheme is based on a concept of topological code discovered by Kitaev [10] and developed in Ref. [6]. In its version, called planar code, qubits are situated on links of a 2D lattice (see Fig. 1). To maintain the encoded quantum information it is enough to measure repeatedly local four-qubit observables of two types - plaquette observable Z_p and star observable X_s :

$$X_s = \otimes_{l \in s} \sigma_l^x, \quad Z_p = \otimes_{l \in p} \sigma_l^z \quad (7)$$

Here s is a star associated with a vertex, and it denotes all links that touch the vertex, while p denotes all links that touch a given plaquette. In Ref. [11] this scheme was applied to long distance communication, and it was analyzed how the distance depends on error rate. However the authors consider communication of logical qubits (i.e. encoded ones). To estimate the fidelity of communicating a physical qubit, or sharing an entangled pairs, we need to complement this analysis with encoding-decoding scheme. Such a scheme was proposed in [6]. However it

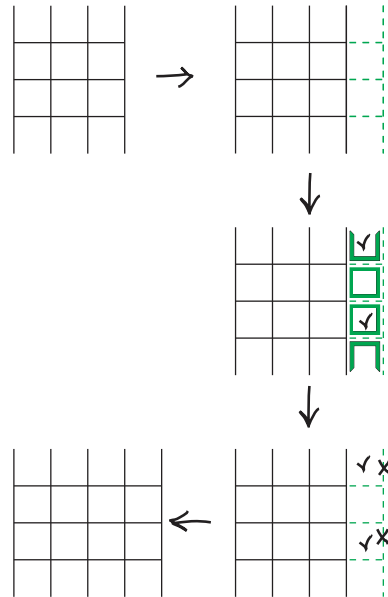


FIG. 2: Appending a column to a code

was relatively complicated, in comparison with simplicity of planar code, and the scheme of maintaining logical qubit. Here we shall propose an encoding-decoding scheme which is as close as possible to the latter one. Namely, we shall use only (i) measurement of X_s and Z_p operators, (ii) measurement and preparation of $|0\rangle, |1\rangle$ and $|\pm\rangle$ basis states (where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$), (iii) bit and phase flips conditioned on measurement outcomes. The latter are not needed in one-shot scenario presented in subsection III B, apart from the very last stage, where correction is applied to the decoded qubit. Even this is not needed if we want to use the scheme for quantum key distribution.

We shall describe below sequential building up the code, as well as a scheme of building it in a single shot.

A. Enlarging and diminishing code

We will present here methods of enlarging code and diminishing it, which are a bit different than the ones in [6].

Appending smooth column The protocol is presented in Fig. 2. We can append a new column to the existing planar code in the following way. First we prepare each of the horizontal and vertical qubits which form that column in a state $|+\rangle$. Next we measure plaquette operators, i.e., tensor product of Z operators on one qubit from the existing code and three (in the case of the highest or the lowest plaquette two) qubits from new column. Finally, we apply bit flip operation to appended external qubits which correspond to plaquettes with nontrivial error syndrome (i.e. when the result of measurement is -1).

Note that this correction procedure is equivalent to the following one. Let us call plaquettes with nontrivial

syndrome as Z-defects. We then join defects with paths of bit-flips in dual lattice. If a single defect is left, we join it with the nearest boundary (which is nothing but applying bit-flip to the external qubit belonging to the plaquette with defect). This correction differs from the above one by some closed loops of bit-flips, which however act trivially on code space.

Before we verify that this procedure works, let us explain in more detail, how to apply it in the situation, where the initial code is just a single qubit. We imagine, that the qubit is represented by a vertical link. Then adding smooth column means to add another vertical link to the right. The above procedure then reduces to preparing this link in state $|+\rangle$, measuring operator $\sigma_x \otimes \sigma_x$ and applying the added qubit σ_z in case of outcome -1 occurs in the measurement.

To see that our procedure transfers encoded state into the same state of a larger code, we need to argue that (i) if the initial state is in the code, the final state belongs to the code too; (ii) the codewords $|0\rangle_L$ and $|1\rangle_L$ are transformed into the codewords of the larger code $|\tilde{0}\rangle_L$, $|\tilde{1}\rangle_L$ (iii) the procedure does not allow to distinguish between the codewords (hence also any superposition of the codewords will be correctly transferred).

Proof of (i). Clearly, the total state of the initial lattice and the appended qubits (prepared in state $|+\rangle$) is eigenvector of operators X_s with eigenvalue $+1$. Since operators Z_p commute with X_s , after measurement, the resulting state is still the eigenstate of all X_s , with the same eigenvalue. Also flipping bits is operation which commutes with X_s , hence the final state is eigenstate of all X_s with eigenvalue $+1$. Thanks to bit flips, the final state is also eigenvector of Z_p 's with eigenvalue $+1$. Therefore it belongs to the code of the enlarged system.

Proof of (ii). A state is a codeword iff it is an eigenstate of the logical operator Z_L to a fixed eigenvalue. We can choose this operator to be on the leftmost vertical line (see caption of Fig. 1). Our manipulations do not touch this line, hence the resulting state is again an eigenstate of this operator with the same eigenvalue.

Proof of (iii). We need to argue, that the value of outcomes of measurements are independent of the codeword. Note, that without changing the statistics, we can first measure the codewords in bit basis. Thus it is enough to argue, that if the measurement of Z_p is applied to a state $|c\rangle$ from the bit basis, the outcomes of measurements are independent of c . To see, that this is the case, note that each Z_p touches one qubit from c and two or three qubits prepared in state $|+\rangle$. We can also premeasure this latter state in bit basis. Thus the outcome is a xor of random bits coming from the latter state with a bit coming from c , hence it is completely independent of c .

In appendix, we give an alternative version of the proof, basing on lemma 2.

Removing a smooth column

In order to remove an external column we measure X operator on each qubit from this column, i.e., we measure X operator on n vertical qubits and $n-1$ horizontal

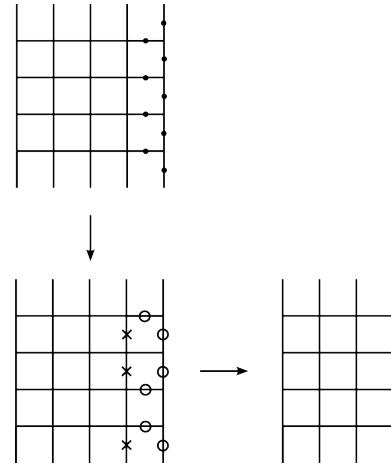


FIG. 3: Removing smooth column. The qubits with solid circles are measured in $|\pm\rangle$ basis. The open circles mark the qubits, which produced outcomes -1 . Phase flips are applied to the crossed qubits.

qubits. Because the measurement of X operator does not reveal the value of Z operator the eigenvalues of the remaining plaquette operators are equal to 1. However the eigenvalues of the new three-qubit star operators X_s , i.e., those which result from four-qubit star operators with one horizontal qubit removed are equal to the result of measurement of X operator on the removed qubit. Hence we apply phase-flip operation to external qubits which correspond to star operators with nontrivial error syndrome. If there are neighboring three-qubit stars, one of them should be corrected, the other not, we have to flip the qubit which does not belong to the latter star. One can ask whether this can be done consistently.

Here is an algorithm which shows that it is indeed the case. Note that the paths of observed -1 's (in direct lattice) end up either on the smooth boundary of the smaller lattice, or on the sharp boundary of the considered column of original lattice. We now join the ends of those paths (or join the ends with either of sharp boundaries) by paths of phase-flips in such a way that the emerging overall configuration of paths is homologically trivial (now in direct lattice). This actually boils down to the following rule: *flip the qubits of the last but one vertical line to the right, provided the corresponding qubit of the last vertical line to the right gave outcome -1 while measured* (see Fig. 3).

Again, it is clear, that this protocol transforms code into a larger code. Moreover, similarly as above, it does not change the value of Z_L . To see that it does not change X_L , take arbitrary horizontal line of qubits in dual lattice. If the measurement of the rightmost qubit gave outcome $+1$, then the value of X_L for the smaller code is the same as the original one, and according to above rule, no qubit from the line is flipped. If the outcome is -1 , the value is opposite, but according to the rule, the last but one qubit to the right is flipped, hence the

original value is restored.

Here there is an alternative reasoning, stated in terms of homology. Let us prove that this protocol indeed maps a codeword of a larger code into corresponding codewords to a smaller code. To this end it is enough to check that, if the initial code is in a state $|c\rangle$ which is a product of $|+\rangle$'s and $|-\rangle$'s then the smaller code will be in a state $|\tilde{c}\rangle$ of the same homology of paths of $|-\rangle$'s. To see it let us write $c = c_1 + c_2$ where c_1 are the paths on a smaller code, and c_2 on the removed part. Denote also by e the flips performed in the protocol. We have that $\tilde{c} = c_1 + e$. Therefore $\tilde{c} + c = c_2 + e$. Our protocol is such that $c_2 + e$ has trivial homology. This means that \tilde{c} and c have the same homology, which ends the proof.

Appending/removing a rough row. This is done in an analogous way, by exchanging $|0\rangle, |1\rangle \leftrightarrow |+\rangle, |-\rangle$ and $X \leftrightarrow Z$ whenever X or Z appear (e.g. in syndrome measurement or logical operators).

B. One shot encoding and decoding

The primitives described in the previous section allow to construct full code starting from a single qubit, recursively by adding a column, then adding a row, then adding a column and so on. However, all operators which we measure commute, and hence, they can be measured simultaneously. This allows us to simplify our encoding. The same concerns decoding. Here we present a scheme with one-shot encoding/decoding.

One shot encoding. The lattice is divided into three parts: lower triangle (green qubits), upper triangle (red qubits), and the qubit to be encoded (black one), see Fig. 4.

The procedure is as follows:

- we measure all X_s which include at least one red qubit (i.e. qubit from upper triangle).
- we measure all Z_p which include at least one green qubit (i.e. qubit from lower triangle).
- we apply phase-flips to red qubits along arbitrarily chosen paths joining the X -defects (stars with where -1 was obtained).
- we apply bit-flips to green qubits along arbitrarily chosen paths joining the Z -defects (plaquettes where -1 was obtained).

Remark. Though our scheme encodes an unknown state, it resembles as closely as possible the procedure of encoding known state given in [6]. E.g. to prepare $|0\rangle_L$ (or $|1\rangle_L$), in that scheme, one prepares first all qubits in state $|0\rangle$ (or $|1\rangle$, resp.), and then measure syndrome of type X . Then one join defects in arbitrary way. In turn, to prepare $|\pm\rangle_L$ state, one proceeds in a dual way: prepares qubits in $|\pm\rangle$ state, and measures Z syndrome. In our scheme, we do these two things at the same time, in two separate triangles.

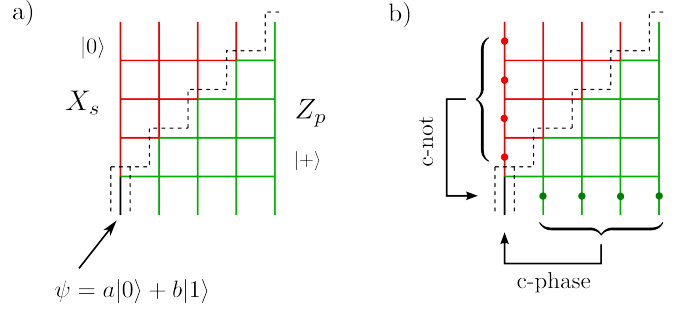


FIG. 4: a) One shot encoding protocol. The lattice is divided into three parts separated by dashed line. The lower triangle - green qubits - will be prepared in $|+\rangle$ states, and all Z_p which touch some green qubits are measured. The upper triangle (red qubits) are measured, and all X_s which touch some red qubits are measured. The black qubit (in the state ψ) located in the left bottom corner is the one to be encoded. The Z -defects and X -defects are annihilated without crossing the dashed line. b) One shot decoding ("single line protocol"): on qubits of the bottom line (apart from the black qubit) bit is measured, and a bit flip to black qubit is applied, when parity is odd. On the qubits of the leftmost line (again, apart from the black qubit) phase is measured, and the phase of black qubit is flipped, when phase parity of odd.

To prove that our encoding works, we shall need a small lemma:

Lemma 2 *Let a system of n qubits be in some bit basis state. Let A be a subsystem. Then measuring $X_A \equiv \bigotimes_{i \in A} \sigma_x^i$ leads to a superposition of two strings: the initial one, and the one flipped by X_A .*

Proof. Let us write $X_A = P_+ - P_-$. Then we have $P_{\pm} = \frac{1}{2}(I \pm X_A)$, which proves the lemma. ■

Proposition 3 *The above encoding procedure, encodes black qubit $\psi = a|0\rangle + b|1\rangle$ into superposition of codewords $a|0\rangle_L + b|1\rangle_L$.*

Proof. Clearly after the above procedure we are in the code, as all defects are removed and therefore all stabilizers are set to $+1$. By lemma 5 it is enough to check that states $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ are correctly encoded. Let us first consider initial states $|0\rangle$ and $|1\rangle$. We then have to show that the value of a chosen logical operator Z is $+1$ or -1 , respectively. We can choose the operator along the leftmost vertical line, which means that we need to check bit parity of this line. In the first stage some X_s operators are measured, then phase flips are applied, and finally Z_p operators are measured. (Note, that no bit-flips are applied to this line.) The phase flips do not affect parity. Using the lemma 2 we obtain that instead of measurements we can check how applications of X_s 's and Z_p 's as unitaries affect the parity. Clearly only application of X_s 's can affect bit values of the line. Since X_s always touch two qubits from the line, they do not change parity. Now, the initial parity is equal to bit value of the

black qubit. This proves that $|0\rangle$ and $|1\rangle$ are mapped into logical states $|0\rangle_L$ and $|1\rangle_L$ of the total code.

The proof that $|+\rangle$ and $|-\rangle$ are correctly transferred is analogous, by examining of phase parity of the lower horizontal line (in dual lattice). ■

One shot decoding. We measure the lowest row of qubits in the basis $|\pm\rangle$ (except of the black qubit), compute parity, and flip phase of black qubit, when the parity is odd.

Then we measure the leftmost column of qubits in $|0\rangle, |1\rangle$ basis, compute parity, and flip the bit of the black qubit when the parity is odd.

Proposition 4 *The above decoding procedure, decodes the superposition of codewords $a|0\rangle_L + b|1\rangle_L$ into the state $\psi = a|0\rangle + b|1\rangle$ of black qubit.*

Proof. To this end we need to show that it sends $|0\rangle_L$ and $|1\rangle_L$ into $|0\rangle$ and $|1\rangle$ respectively. The proof that $|\pm\rangle_L$ is sent into $|\pm\rangle$ is the same. Again, by the lemma 5, having correctly transferred those four states, we obtain that all states are also correctly transferred. If the code is in the state $|0\rangle_L$ then the left-most vertical line if measured would give even number of 1's. Thus, if we measure all qubits from the line but the black one, then the measured parity must be equal to bit of the black qubit. But we want to get $|0\rangle$, i.e. trivial parity. Hence we have to apply bit-flip, if the measured parity is nontrivial. Same reasoning works for initial state $|1\rangle_L$: the parity of the whole line is odd, thus if we want to have the bit value of the black qubit equal to that parity, we need to flip the black qubit, when the parity of other qubits is odd. ■

IV. ENCODING AS TELEPORTATION

We shall now show, that encoding a qubit in unknown state, is equivalent to teleportation. Let us first present teleportation in terms of stabilizer formalism. To this end, recall [12] that common eigenstates of operators X_1X_2 and Z_1Z_2 are Bell states. Hence teleportation can be viewed as follows. Let qubit number 1 be the qubit to be teleported (hold with Alice) and the qubits number 2 and 3 be the ones in maximally entangled state (qubit 2 with Alice and qubit 3 with Bob). Then teleportation is obtained by the following protocol: first X_1X_2 is measured. If the outcome is -1 , then transformation Z_2Z_3 is performed. Then Z_1Z_2 is measured, and, if the outcome is -1 transformation X_2X_3 is performed. These operations transform qubit 3 to initial state of qubit 1 and qubits 1 and 2 to initial Bell state of qubits 2 and 3.

Now, let us consider our single shot encoding procedure. Note that we can first measure all the syndromes that do not touch the physical qubit. Then the remaining part of the procedure of encoding consists of the following two stages: (i) measuring syndromes that touch physical qubit (ii) removing the obtained defects. More precisely, we measure a single syndrome Z_p which touches

our physical qubit. If the syndrome is nontrivial, then we move it away by applying bit-flips to lowest path of qubits (in dual lattice). We then measure single syndrome X_s which touches the physical qubit, and if the syndrome is nontrivial, we apply phase flips to the left-most vertical line of qubits (in original lattice).

Let us now show that this is teleportation. To this end we have to determine three qubits. The first stage prepares a two-qubit code: one qubit is described by logical operators X_2, Z_2 and the other by X_3, Z_3 (see Fig. 5). These two qubits will be qubits 2 and 3 and, because

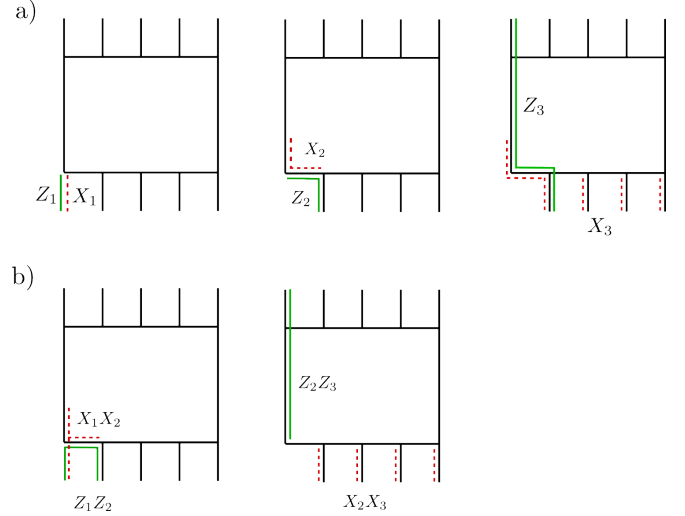


FIG. 5: Single shot encoding as teleportation. The black lattice symbolizes two-qubit code resulting from measuring all syndromes but the ones touching the physical qubits. a) three qubits needed for teleportation b) two stages of encoding can be interpreted as operations that perform teleportation.

the code is a common eigenstate of operators X_2X_3 and Z_2Z_3 , the qubits turn out to be in maximally entangled state. Our physical qubit is the one to be teleported, i.e. labeled by 1, with associated operators X_1, Z_1 . The operators defining the three qubits are collected on Fig. 5 a). Then, we notice that the operators X_1X_2 and Z_1Z_2 take exactly the form of syndromes Z_p and X_s touching the physical qubits, thus corresponding to the stage (i) above, while X_2X_3 and Z_2Z_3 are exactly flipping bit and phase respectively along the appropriated paths, as done in stage (ii).

Decoding is also teleportation, in even more traditional form: we measure X_2X_3 and Z_2Z_3 (Bell measurement), and correct suitably the qubit 1 (cf. Fig. 4).

V. NOISY SCENARIO

So far we have assumed that syndrome measurement is ideal. In this section we shall present simulations of noisy case, where also the syndrome readout is nonideal. We shall closely follow the original ideas of [6] and the implementation of [13]. Our numerical simulations have

illustrative character, hence we have decided to consider a simpler scenario, where errors on syndromes do not propagate back to the code. I.e., we imagine that a syndrome is measured in a noiseless way, and the classical outcome of syndrome measurement is flipped with some probability.

To find what is the fidelity of encoding-decoding stage, due to symmetry of the problem, it is enough to check fidelity for $|0\rangle$ state. This implies the same bounds for $|1\rangle$, $|+\rangle$ and $|-\rangle$, and therefore implies e.g., high average fidelity for arbitrary state of qubit according to lemma 5.

To estimate the above fidelity, we need to generate a random error on lower triangle and error with probability p on upper triangle in the first step, and in subsequent steps errors with probability p on the whole plane. In each step we measure Z_p syndrome. Next, we apply the perfect matching algorithm, in such a way, that we do not allow to flip the black qubit, on the basis of results of the first step of the protocol (as this first stage is encoding step). Finally we obtain some configurations of zeros and ones. We apply error with probability p to those bits (this simulates error of reading them out). Then we choose various paths (in dual lattice) connecting the black qubit and the right boundary (ideally one should take all possible paths, but in practice, some smaller number may be enough). We compute parity of those paths on the part excluding the black qubit. Then we take majority of those parities, and flip the bit of black qubit, if the majority is 1. In the plots we consider two decoding cases: (i) in first case we consider only the single lower line of qubits (except the black qubit), we call this decoding scheme the *line decoding*, (ii) in the second scenario we consider every path starting on the east edge and going in each step either to the left or to the bottom until it reaches the black qubit (but in such a way to stay in the lower triangle), we then take the majority vote of all those paths, we call this method decoding scheme the *multiline decoding*.

We present the results of the simulations on Fig. 6–10. On all of the plots axis x represents probability of error p (same probability for error on qubit and error on syndrome, unless no error on syndrome specified) and axis y represents estimated probability of successful decoding. The probability is estimated numerically by computing the fraction of n runs for which decoding succeeds ($n = 10^4$ if not explicitly specified). Each of n runs consists of encoding the qubit into the code (7×8 code is used unless other specified) storing it in the code for $k = 100$ steps and decoding using line decoding (unless multiline decoding explicitly specified). The run is considered successful if the qubit is properly decoded. If ‘no encoding’ is specified this means that the run starts with the qubit properly encoded into the code and after k steps of the algorithm the perfect decoding is used.

On Fig. 8 we use a lower bound for the probability of successful storing of a qubit [6] in an $N \times M$ code for k

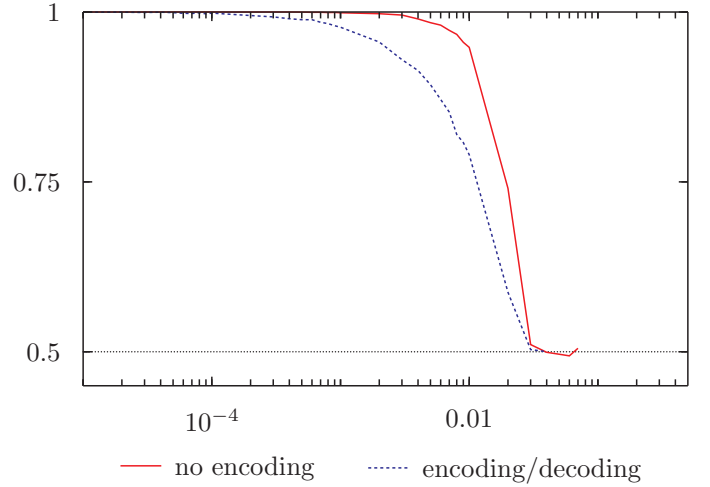


FIG. 6: Comparison of estimated probability of proper decoding between encoding and line decoding, and no encoding and perfect decoding.

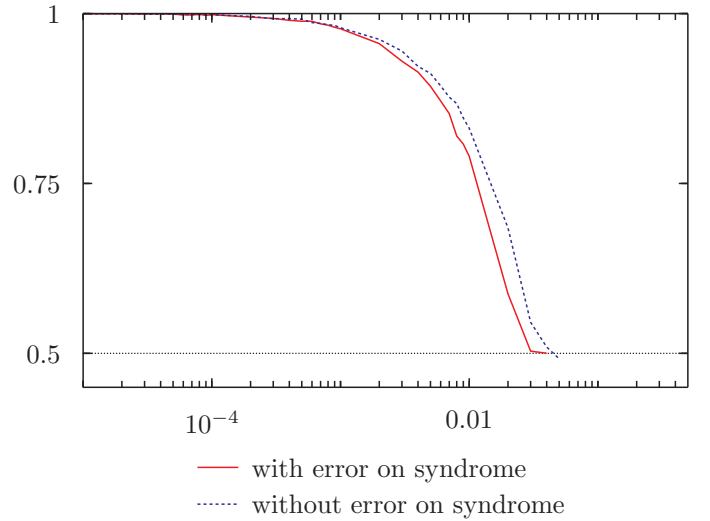


FIG. 7: Comparison of estimated probability of proper decoding between errors on both qubits and syndrome, and errors only on qubits.

steps of the algorithm

$$p_s^{N \times M}(p) \geq 1 - NMk \frac{\alpha^{\max(N,M)}}{1 - \alpha} \quad (8)$$

where k is the number of steps of the algorithm (in our simulations we have $k = 100$) and p is the probability of error same probability for errors on the qubits and on the syndrome, and

$$\alpha = 6 \cdot 2 \cdot \sqrt{(1-p)p}. \quad (9)$$

The numerical simulations show that for so small codes, the protection is not monotonic with size of the code. The best one is 7×8 code, as the larger codes become better only for value of p , for which the probability

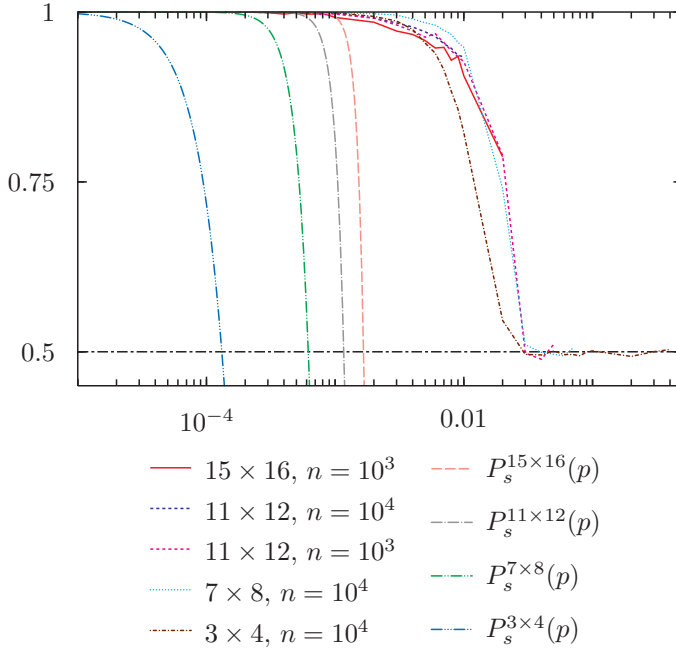


FIG. 8: Comparison of estimated probability of proper decoding for no encoding and perfect decoding and different code sizes.

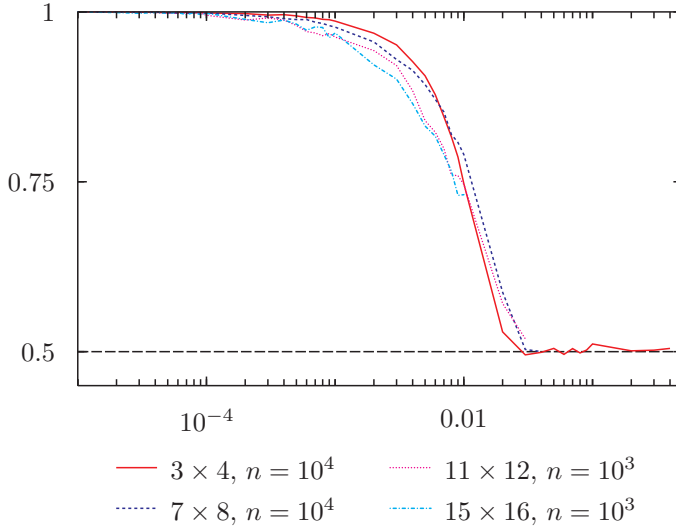


FIG. 9: Comparison of estimated probability of proper decoding for encoding and line decoding and different code sizes.

of successful decoding is small. This behaviour is due to the finite size effect.

VI. IMPLICATIONS FOR ENTANGLEMENT PERCOLATION

In entanglement percolation [4], the idea is that in each node one performs operation consisting of constant number of elementary operations, i.e. it does not depend on

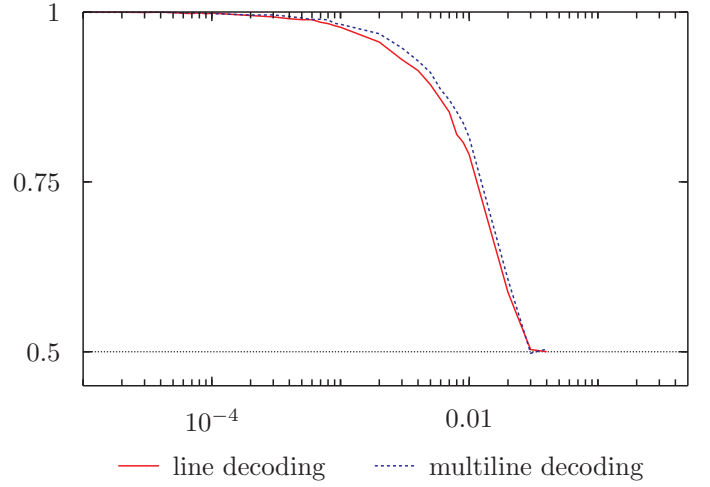


FIG. 10: Comparison of estimated probability of proper decoding between line decoding and multiline decoding.

the size of the network. The task is then to share entanglement between two distant nodes with a fidelity F , which does not decay when the network is enlarged.

According to [1] if we have computation scheme of dimension d , which allows to preserve a qubit in time, then we can translate it into network of $d + 1$ that allows to share entanglement between two nodes of network. Our results now imply, that in 2D EPR-network a node-to-node entanglement percolation is possible. In other words, if in the 2D square network the neighboring nodes share EPR pair, two nodes can share entangled pair with a fidelity that scales reasonably with the error rate. Namely, $F = F_0(1 - \exp(-ap))$ where $F_0 \geq \exp(-vp)$, with v, a being absolute constants, p is error rate. The factor F_0 comes from encoding, the second factor - from storing the encoded state.

Since our scheme based on 1D architecture for fault-tolerant quantum computing using concatenated codes, it is quite complicated. We have therefore also proposed a 3D network, which bases on 2D Kitaev code. The communication scheme for encoded state was analyzed in [11]. Here we have complemented it with a simple scheme of encoding/decoding an unknown state, which allows to obtain node-to-node entanglement percolation. Our scheme, similarly as that of [1] needs three dimensions. Two of them are only logarithmic in the distance between the nodes which want to share entanglement. Our protocol is more uniform, because the only operations are syndrome measurements for encoding, Pauli measurements for decoding and entanglement swapping. Indeed, we do not need to perform the flips in the encoding scheme: it is enough to store this information classically.

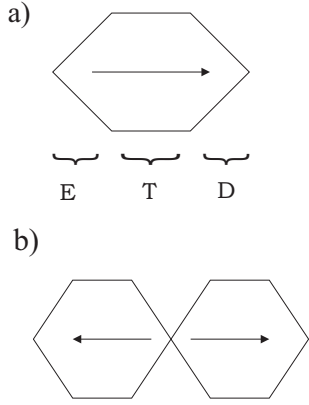


FIG. 11: Transmitting qubits vs sharing ebits. By E,D, T we denote encoding, decoding and transmitting.

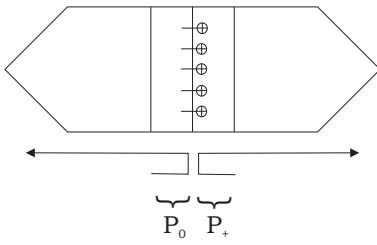


FIG. 12: Sharing e-bits without unknown-state encoding stage. Here $P_{0,(+)}$ mean the stage of preparing logical state $|0\rangle_L$ ($|+\rangle_L$).

A. Sharing node-to-node entanglement

In order to transmit a qubit, it is enough to change time into one more space direction as in [1]. To share entanglement, we need to propagate two qubits in opposite time directions. If we translate it into space, we obtain the following scheme: in one node an EPR pair is prepared, and each of two qubits is transmitted towards one of two nodes which we want to share entanglement (see Fig. 11).

There is an alternative scheme of sharing entanglement, which does not need encoding, but only decoding (see Fig. 12). The idea is the following: we shall not start from a qubit, which we then want to transmit. Rather, we shall prepare known encoded states. On one 2D plane we prepare $|0\rangle_L$ state (which in percolation picture will use up 3D network). As described in Sec. III B, this amounts to prepare all qubits in state $|0\rangle$ and measure repeatedly star and plaquette observables, and write down syndrome. On another 2D plane we shall prepare in an analogous way $|+\rangle_L$ state. Then c-nots will be applied bit-wise between the planes, so that we shall obtain EPR state between two logical qubits. Then we transmit the qubits in opposite directions, and they are localised into two single qubits by our decoding method, described in previous section. The same of course can be done in the case of 2D network.

Finally, one should be aware, that the scheme of quantum communication over networks inherits the problems of applicability of fault tolerant schemes to the Hamiltonian description of interaction of the system with environment see e.g. [14–19] or a recent discussion [20].

VII. ACKNOWLEDGMENT

We would like to thank Robert Alicki, Ryszard Horodecki and Andrew Steane for helpful discussion. This paper is supported by EC IP QESSENCE and by the Polish Ministry of Science and Higher Education grant N N202 231937. P. M. and A. P. are supported by the International PhD Project "Physics of future quantum-based information technologies": grant MPD/2009-3/4 from Foundation for Polish Science. Part of this work was done in National Quantum Information Centre of Gdańsk.

Appendix

1. Some proofs

Alternative proof of validity of the procedure of enlarging codes by adding columns or rows

- *The procedure transforms code into code.* Consider e.g. adding columns. We have to ensure that after the procedure all X_s and Z_p operators have sign +1. When we attach a column with all qubits prepared in state $|+\rangle$, the operators X_s on larger code have clearly value +1. Let us argue, that after measuring operators Z_p the operators X_s keep this sign. Let us denote the initial state of the code tensored by the added column in state $|+\rangle$ by ψ . We have that $\psi = \sum_{c'} |c'\rangle_{\pm}$ where c' are configurations of $+$, $-$'s. Clearly all the configurations in the sum constitute closed paths of $-$'s (i.e. they are either constitute loops or end up at a boundary). Let us now measure a single Z_p on that state, and suppose we have obtained some outcome. According to lemma 2, for this particular outcome each $|c'\rangle$ is transformed into superposition of $|c'\rangle$ and $Z_p|c'\rangle$. Now, application of Z_p flips sign of qubits belonging to a closed path, hence $Z_p|c'\rangle$ has still only closed paths of $-$'s.

This proves that X_s operators of the enlarged system have all +1 sign. The operators Z_p also do, because in the second stage of the procedure we perform suitable bit-flips, which remove Z -defects.

- *The procedure transfers logical $|\pm\rangle$ states into those of larger code.* Suppose that the initial state of smaller code is $|+\rangle_L$. Then the initial state of the total system is a superposition of states $|c'\rangle$ with c' being homologically trivial configuration of $+$ and

–’s. We have noticed above, that application of Z_p to $|c'\rangle$ does not introduce X_s defects. However, even more is true: it preserves homology of paths of –’s. Moreover the subsequent bit-flips change only phase of $|c'\rangle$. Therefore, the final state is also a superposition of homologically trivial $|c'\rangle$ ’s. Since the final state belongs to the code, it must be $|\tilde{+}\rangle_L$ (where tilde is used to denote state from enlarged code).

- *The procedure transfers logical $|0\rangle, |1\rangle$ states into those of larger code.* Here the reasoning is the same as in the main text. E.g. for column addition all operations are far from left boundary, hence the homology of bit-strings cannot change. Therefore, we end up with superposition of bitstrings of the same homology as original, hence, since we are in the code, the final state must be $|0\rangle$ or $|1\rangle$ logical

state, for initial logical state $|0\rangle, |1\rangle$, respectively.

Lemma 5 [21] *Consider a completely positive map Λ on single qubit, and define $F(\psi) = \langle \psi | \Lambda(|\psi\rangle\langle\psi|) | \psi \rangle$. Let F_x, F_z be given by*

$$F_x = \frac{1}{2}(F(|0\rangle) + F(|1\rangle)) \quad F_z = \frac{1}{2}(F(|+\rangle) + F(|-\rangle)) \quad (10)$$

where $|0\rangle, |1\rangle$ are eigenstates of σ_z and $|\pm\rangle$ are eigenstates of σ_x . Then:

$$\overline{F} \geq F_x + F_z - 1 \quad (11)$$

where $F = \int F(\psi) d\psi$ is average fidelity, over uniformly chosen input states.

-
- [1] S. Perseguers, L. Jiang, N. Schuch, F. Verstraete, M. D. Lukin, J. I. Cirac, and K. G. H. Vollbrecht, *Physical Review A* **78**, 062324 (2008), arXiv:0807.0208.
 - [2] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, *Phys. Rev. Lett.* **81**, 5932 (1998).
 - [3] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, *Nature* **414**, 413 (2001), arXiv:quant-ph/0105105.
 - [4] A. Acin, I. Cirac, and M. Lewenstein, *Nat. Phys.* **3**, 256 (2007), arXiv:quant-ph/0612167.
 - [5] A. M. Stephens, A. G. Fowler, and L. C. L. Hollenberg, *QIC* **8**, 330 (2008), arXiv:quant-ph/0702201.
 - [6] E. Dennis, A. Kitaev, A. Landahl, and J. Preskill, *J. Math. Phys.* **43**, 4452 (2002), quant-ph/0110143.
 - [7] R. Raussendorf, S. Bravyi, and J. Harrington, *Phys. Rev. A* **71**, 062313 (2005), arXiv:quant-ph/0407255.
 - [8] S. Perseguers, *Phys. Rev. A* **81**, 012310 (2010), arXiv:0910.1459.
 - [9] D. Aharonov and M. Ben-Or, *Fault tolerant quantum computation with constant error* (1996), quant-ph/9611025.
 - [10] A. Y. Kitaev, *Annals Phys.* **303**, 2 (2003), quant-ph/9707021.
 - [11] A. G. Fowler, D. S. Wang, C. D. Hill, T. D. Ladd, R. van Meter, and L. C. L. Hollenberg, *Phys. Rev. Lett.* **104**, 180503 (2010), 0910.4074.
 - [12] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
 - [13] A. G. Fowler, A. M. Stephens, and P. Groszkowski, *High threshold universal quantum computation on the surface code* (2008), arXiv:0803.0272.
 - [14] R. Alicki, M. Horodecki, P. Horodecki, and R. Horodecki, *Phys. Rev. A* **65**, 062101 (2002), quant-ph/0105115.
 - [15] R. Alicki, *Quantum error correction fails for Hamiltonian models* (2004), arXiv:quant-ph/0411008.
 - [16] B. M. Terhal and G. Burkard, *Phys. Rev. A* **71**, 012336 (2005), quant-ph/0402104.
 - [17] R. Alicki, *Comments on “fault-tolerant quantum computation for local non-markovian noise”* (2004), quant-ph/0402139.
 - [18] R. Alicki, D. A. Lidar, and P. Zanardi, *Phys. Rev. A* **73**, 052311 (2006), arXiv:quant-ph/0506201.
 - [19] D. Aharonov, A. Kitaev, and J. Preskill, *Phys. Rev. Lett.* **96**, 050504 (2006), quant-ph/0510231.
 - [20] *Perpetual motion of the 21st century?*, URL <http://rjlipton.wordpress.com/2012/01/30/perpetual-motion-of-the-21st-century>.
 - [21] H. Hofmann, *Phys. Rev. Lett.* **94**, 160504 (2005), quant-ph/0411011.